UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/518,639	12/20/2004	Nathalie Feyt	1032326-000288	4953

21839 7590 02/05/2010
BUCHANAN, INGERSOLL & ROONEY PC
POST OFFICE BOX 1404
ALEXANDRIA, VA 22313-1404

EXAMINER	
SU, SARAH	

ART UNIT	PAPER NUMBER
2431	

NOTIFICATION DATE	DELIVERY MODE
02/05/2010	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

ADIPFDD@bipc.com
offserv@bipc.com

Office Action Summary	Application No.	Applicant(s)	
	10/518,639	FEYT ET AL.	
	Examiner	Art Unit	
	Sarah Su	2431	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *20 November 2009*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-10 and 12-19* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-10, 12-19* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 20 November 2009 has been entered. In this amendment, claim 1 has been amended, claim 11 has been canceled, and claim 19 has been added.

2. Claims 1-10 and 12-19 are presented for examination.

Response to Arguments

3. Applicant's arguments filed 20 November 2009 have been fully considered but they are not persuasive.

As to claim 11 (currently incorporated into claim 1), it is argued by the applicant that Hopkins does not disclose that the product of two of the numbers is evaluated to determine whether its length is equal to a given value l. The examiner respectfully disagrees. Hopkins discloses that very large modulus numbers having a long length are now being used in cryptographic keys n order to increase security levels and that in the classic 2-prime RSA encryption algorithm, each of the prime factors p and q has a length which is equal to half the bit length of the modulus n (0018, lines 8-18). Hopkins also discloses that the prime numbers are searched according to associated length

parameters (0043, lines 11-12). Therefore, since the generated primes are checked to find a prime of a certain length, the desired length of the modulus is essentially being search since the length of p and q must be half of the length of n.

Further as to claim 11 (currently incorporated into claim 1), it is argued by the applicant that Hopkins does not disclose that a pair of selected prime numbers is evaluated for verification. The examiner respectfully disagrees. Hopkins discloses that the modulus is generated from the product of an associated number k of randomly generated distinct and suitable prime number values wherein k>=1 (0083, lines 5-11).

As to claim 12, it is argued by the applicant the Hopkins does not receive a value for the length of the modulus from some external source. The examiner respectfully disagrees. Hopkins discloses that a security module prime generation unit generates prime number values and has a port communicatively coupled with a port of the server computing system via a server system bus (0093, lines 4-9) and that N, e, and d are transmitted via the bus to the server computing system (52, Figure 3). Therefore, since e is being transmitted, the length of e is also being transmitted.

Claim Rejections - 35 USC § 101

4. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

5. Claims 1-10 and 16-18 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

Claims 1-10 and 16-18 are rejected under 35 U.S.C. 101 as not falling within one of the four statutory categories of invention. While the claims recite a series of steps or acts to be performed, a statutory "process" under 35 U.S.C. 101 must (1) be tied to particular machine, or (2) transform underlying subject matter (such as an article or material) to a different state or thing. See page 10 of In Re Bilski 88 USPQ2d 1385. The instant claims are neither positively tied to a particular machine that accomplishes the claimed method steps nor transform underlying subject matter, and therefore do not qualify as a statutory process. The generating electronic keys method including steps of calculating, storing, obtaining, retrieving, and verifying is broad enough that the claim could be completely performed mentally, verbally or without a machine nor is any transformation apparent. It is noted that the preamble of claim 1 indicates that a public-key cryptography method uses an electronic device, but the method of generating electronic keys is not tied to a particular machine. Further, the electronic device of the preamble is not recited in the body of the claim.

Claim Rejections - 35 USC § 102

6. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

7. Claims 1-5, 12, 13, 15, 16, and 19 are rejected under 35 U.S.C. 102(e) as being anticipated by Hopkins et al. (US 2005/0190912 A1 and Hopkins hereinafter).

As to claim 1, Hopkins discloses a system and method for pre-computing and storing multiple cryptographic keys, the system and method having:

calculating pairs of prime numbers (p, q) or values representative of pairs of prime numbers, this calculation being independent of knowledge of a pair of values (e, l) in which e is the public exponent and l is the length of the key of the cryptography method (0038, lines 6-7),

storing the pairs or values thus obtained (0038, lines 7-10);

obtaining values for e and l (0036, lines 2-9)**;**

retrieving a pair of prime numbers (p, q) or a value representative of said pair of prime numbers, stored in step A (0038, lines 11-12)**;**

verifying the following conditions for said pair of prime numbers:

(i) p-1 and q-1 are prime numbers with the obtained value for e (0063, lines 1-6)

(ii) N=p*q is an integer of given length l (0018, lines 12-18; 0043, lines 11-12)**,**

if the pair (p, q) does not satisfy conditions (i) and (ii), retrieving another pair of prime numbers and repeating the verification until a retrieved pair is suitable (0063, lines 4-6)**;**

calculating a key d from the retrieved pair (p, q) that is determined to be suitable (0068, lines 1-4).

As to claim 2, Hopkins discloses:

> **wherein step A-1) comprises calculating pairs of prime numbers (p, q) without knowledge of the public exponent e or of the length l of the key, using a parameter Π** (i.e. n) **which is the product of small prime numbers** (i.e. p_1, p_2, ...) (0057, line 16)**, so that each pair (p, q) has a maximum probability of being able to correspond to a future pair (e,l) and can make it possible to calculate the key d** (0068, lines 1-4)**.**

As to claim 3, Hopkins discloses:

> **wherein the calculation of step A-1) also takes account of the fact that e has a high probability of forming part of the set {3, 17, . . . , 2^{16}+1}** (0127, lines 3-5)**, and using a seed σ in the calculation which makes it possible to calculate a representative value constituting an image** (i.e. prime number value) **of the pairs (p, q)** (0041, lines 1-4)**.**

As to claim 4, Hopkins discloses:

> **wherein the storage step A-2) comprises storing the image** (i.e. cryptographic parameters) **of the pairs** (0035, lines 23-24)**.**

As to claims 5 and 16, Hopkins discloses:

wherein step A-1) comprises calculating pairs of prime numbers (p, q) for different probable pairs of values (e,l) (0035, lines 5-8).

As to claim 12, Hopkins discloses:

communication means for receiving at least one pair of values (e,l) (52, Figure 3);

a memory for storing the results of: calculating pairs of prime numbers (p,q) or values representative of pairs of prime numbers, this calculation being independent of knowledge of the pair of values (e,l) in which e is a public exponent and l is the length of the key of the cryptography method (0038, lines 6-10);

a program for calculating a key d from the stored results and knowledge of a received pair of values (e,l) (0068, lines 1-4).

As to claim 13, Hopkins discloses:

a calculation means configured to calculate said results stored in memory, the calculation of said results being separate in time from the calculation of the key d (0042, lines 2-4; 0068, lines 1-4).

As to claim 15, Hopkins discloses:

where said object is a chip card (0094, lines 1-9, 13-15).

As to claim 19, Hopkins discloses:

in a computing resource (i.e. prime generating unit) **external to said electronic device** (i.e. server computing system) (44, 50, 52, Figure 2):

calculating pairs of prime numbers (p, q), or values representative of said pairs of prime numbers, independently of the values for e and l (0038, lines 6-7)**, and**

storing the pairs of prime numbers, or values, in a memory of the electronic device (0038, lines 7-10)**;**

in said electronic device:

obtaining values for e and l (0036, lines 2-9)**;**

retrieving a pair of prime numbers (p, q), or a value representative of said pair of prime numbers, from said memory (0038, lines 11-12)**;**

verifying the following conditions for said pair of prime numbers:

(i) p-1 and q-1 are prime numbers with respect to the value for e (0063, lines 1-6)**, and**

(ii) N=p*q is an integer of length l (0018, lines 12-18; 0043, lines 11-12)**,**

if the pair (p, q) does not satisfy conditions (i) and (ii), retrieving another pair of prime numbers from said memory and repeating the verification steps until a retrieved pair is determined to meet the conditions (0063, lines 4-6)**;**

calculating a key d in accordance with the value for e and a retrieved pair that is determined to meet the conditions (0068, lines 1-4).

Claim Rejections - 35 USC § 103

8. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

9. Claims 6, 8-10, 14, 17, and 18 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hopkins as applied to claims 1, 3, 5, and 13 above, and further in view of Futa et al. (US Patent 7,130,422 B2 and Futa hereinafter).

As to claim 6, Hopkins fails to specifically disclose:

wherein the parameter Π contains the values 3, 17.

Nonetheless, this feature is well known in the art and would have been an obvious modification of the teachings disclosed by Hopkins, as taught by Futa.

Futa discloses a system and method for prime number generation for information security, the system and method having:

wherein the parameter Π (i.e. R) **contains the values 3, 17** (i.e. small primes, L_1, L_2,...) (col. 9, line 43; col. 10, line 8). The examiner asserts that because Futa discloses that the parameter Π consists of small prime numbers, then the numbers 3 and 17 may be included because they can be considered small prime numbers.

Given the teaching of Futa, a person having ordinary skill in the art at the time of the invention would have readily recognized the desirability and advantages of modifying

the teachings of Hopkins with the teachings of Futa by using small primes. Futa recites motivation by disclosing that the computational complexity of generating a 16 bit or 32 bit prime is much smaller than generating a 64 bit prime (col. 5, lines 58-60). It is obvious that the teachings of Futa would have improved the teachings of Hopkins by using a parameter containing small primes in order to reduce computational complexity.

As to claims 8, 14 and 17, Hopkins discloses:

1) calculating parameters v and w from the following relations and storing them:

$v=\sqrt{2^{2lo-1}}/\Pi$

$w=2^{2lo}/\Pi$

in which Π (i.e. n) **is stored and corresponds to the product of the f smallest prime numbers, f** (i.e. k) **being selected such that $\Pi \leq 2^{Bo}$** (i.e. 2^{L}) (0057, line 16; 0062, line 4)**;**

3) selecting and storing a prime number k of short length compared to the length of an RSA key within the range of integers {0, . . ., Π-1}, (k, Π) being co-prime (0057, lines 10-12)**.**

Hopkins fails to specifically disclose:

2) selecting a number j within the range of integers {v, ... , w-1} and calculating l=jΠ;

4) calculating q;

5) verifying that q is a prime number, if q is not a prime number then:

a) taking a new value for k using the following relation: k=a k (mod Π); a belonging to the multiplicative group Z^*_{Π} of integers modulo Π;

b) repeating the method from step 4).

Nonetheless, these features are well known in the art and would have been an obvious modification of the teachings disclosed by Hopkins, as taught by Futa.

Futa discloses:

2) selecting a number j within the range of integers {v, … , w-1} and calculating l=jΠ (i.e. l=R, j=R', Π =L1×L2×…) (col. 9, lines 54-56; col. 10, line 8);

4) calculating q (i.e. P_a/P_b) **=k+l** (col. 8, lines 56-57, 62-64; col. 10, lines 10, 41-43);

5) verifying that q is a prime number, if q is not a prime number then:

a) taking a new value for k using the following relation: k=a k (mod Π); a belonging to the multiplicative group Z^*_{Π} of integers modulo Π;

b) repeating the method from step 4) (col. 10, lines 25-28).

Given the teaching of Futa, a person having ordinary skill in the art at the time of the invention would have readily recognized the desirability and advantages of modifying the teachings of Hopkins with the teachings of Futa by calculating parameters that are used to determine prime numbers for an RSA-type cryptographic system. Hopkins recites motivation by disclosing that the prime numbers must be distinct and suitable for use in the multi-prime cryptographic system (0058, lines 6-9). It is disclosed that the composite number n provides a modulus for encoding and decoding operations (0058,

lines 1-2) and that the prime numbers must fall in a certain range, which, alternatively, ensures that the prime numbers and exponent are relatively prime (0063, lines 1-4). It is obvious that the teachings of Hopkins would have been improved by the teachings of Futa by calculating and using parameters for determining prime numbers in such a way that would ensure distinctness and suitability in the system.

As to claim 9, Hopkins discloses:

> **wherein the numbers j and k can be generated from the seed σ stored in memory** (0041, lines 1-6)**.**

As to claims 10 and 18, Hopkins fails to disclose:

> **where the prime number p is generated by repeating all the above sub-steps while replacing q with p and replacing l_o with l-l_o.**

Nonetheless, this feature is well known in the art and would have been an obvious modification of the teachings disclosed by Hopkins, as taught by Futa.

Futa discloses:

> **where the prime number p is generated by repeating all the above sub-steps while replacing q with p and replacing l_o** (i.e. L_{enq}) **with l-l_o** (i.e. L_{enq}') (col. 8, lines 55-57, 61-64; col. 9, lines 19-25)**.** The examiner asserts that because Futa discloses that the prime numbers p_a and p_b are generated using the same unit, then they can be said to be generated using the same steps.

Given the teaching of Futa, a person having ordinary skill in the art at the time of the invention would have readily recognized the desirability and advantages of modifying the teachings of Hopkins with the teachings of Futa by calculating parameters that are used to determine prime numbers for an RSA-type cryptographic system. Please refer to the motivation recited above with respect to claims 8, 14, and 17 as to why it is obvious to apply the teachings of Futa to the teachings of Hopkins.

10. Claim 7 is rejected under 35 U.S.C. 103(a) as being unpatentable over Hopkins in view of Futa as applied to claim 1 above, and further in view of Matyas (US Patent 4,736,423).

As to claim 7, Hopkins in view of Futa fails to specifically disclose:

> **wherein step A-1) comprises an operation of compressing the calculated pairs (p,q) and step A-2) comprises storing the compressed values thus obtained.**

Nonetheless, this feature is well known in the art and would have been an obvious modification of the teachings disclosed by Hopkins in view of Futa, as taught by Matyas. Matyas discloses a system and method for reducing RSA crypto variable storage, the method having:

> **wherein step A-1) comprises an operation of compressing the calculated pairs (p,q) and step A-2) comprises storing the compressed values thus obtained** (col. 8, lines 65-68; col. 9, lines 1-2)**.**

Given the teaching of Matyas, a person having ordinary skill in the art at the time of the invention would have readily recognized the desirability and advantages of modifying the teachings of Hopkins in view of Futa with the teachings of Matyas by providing for compression of the numbers and storing the result. Matyas recites motivation by disclosing that efficiently storing parameters required for public key algorithms (through a method such as compression) would allow the system to be implemented where storage is limited (such as a magnetic strip card) (col. 3 lines 55-58). It is obvious that the teachings of Matyas would have improved the teachings of Hopkins in view of Futa by compressing parameters used in public key algorithms in order to save space so that the algorithm may be used in conditions where the storage is limited.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Sarah Su whose telephone number is (571) 270-3835. The examiner can normally be reached on Monday through Friday 7:30AM-5:00PM EST..

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, William Korzuch can be reached on (571) 272-7589. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Sarah Su/
Examiner, Art Unit 2431

/Christopher A. Revak/
Primary Examiner, Art Unit 2431